Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Siete, Internet a telekomunikácie
Systémy na detekciu/prevenciu prienikov

Ladislav Hudec

2013

KPMG
cutting through complexity™

Princípy detekcie a prevencie prienikov

- **Detekcia prienikov** – je proces monitorovania udalostí v počítačovom systéme alebo v sieti a ich analyzovania na príznaky možných incidentov, ktoré sú porušením alebo bezprostrednou hrozbou porušenia **politík počítačovej bezpečnosti**, **politík akceptovateľného použitia** alebo **štandardných bezpečnostných praktík**.
  - Incidenty majú mnoho príčin, ako je škodlivý kód (napr. červy, vírusy), útočníci získajú neoprávnený prístup do systémov z Internetu a tiež oprávnení používatelia systémov, ktorí zneužívajú svoje práva alebo sa pokúšajú získať ďalšie povolenia, na ktoré nie sú autorizovaní.
- **Systém detekcie prienikov (IDS – Intrusion Detection Systém)** – je softvér, ktorý automatizuje proces detekcie prienikov.
- **Systém prevencie prienikov (IPS – Intrusion Prevention System)** - je softvér, ktorý má všetky schopnosti systému detekcie prienikov a je schopný pokúsiť sa zastaviť možné incidenty.
- IDS a IPS technológie ponúkajú mnoho rovnakých možností a ich administrátori môžu zablokovať preventívne funkcie v produktoch IPS, čím spôsobia, že fungujú ako systémy IDS.
- **Použitie IDPS technológií** - Tieto technológie sú primárne určené na identifikáciu možných incidentov:
  - IDPS môže detegovať úspešnú kompromitáciu systému útočníkom, ktorý využil slabinu systému. IDPS potom môže oznámiť incident bezpečnostnému manažérovi, ktorý okamžite začne aktivity reakcie na incident, aby sa minimalizovala škoda spôsobená incidentom. IDPS ďalej môže vytvoriť **informačný záznam**, ktorý je využitý na riešenie incidentu.
  - Veľa IDPS môže byť konfigurovaných tak, že **rozpozná porušenie bezpečnostnej politiky**. Napríklad niektoré IDPS môžu byť konfigurované nastaveniami podobnými ako bezpečnostná brána, ktoré IDPS umožnia identifikovať sieťovú premávku porušujúcu politiku bezpečnosti spoločnosti alebo politiku akceptovateľného použitia.
  - Niektoré IDPS môžu **monitorovať prenos súborov a identifikovať možné podozrivé prenosy**, napríklad kopírovanie rozsiahlej databázy na používateľský laptop.
  - Veľa IDPS môžu identifikovať prieskumné aktivity útočníka, ktoré môžu indikovať bezprostredný útok. Príkladom takýchto prieskumných aktivít je **skenovanie portov na webovom serveri**. IDPS môže blokovať takýto prieskum a upovedomiť bezpečnostného administrátora.

Princípy detekcie a prevencie prienikov

- **Použitie IDPS technológií** – okrem identifikovania incidentu a podpory reakcie na incident, môže byť technológia IDS použitá aj na:
  - **Identifikáciu problémov bezpečnostnej politiky** - IDPS môže poskytnúť istý stupeň riadenia kvality implementácie bezpečnostnej politiky. Napríklad IDPS si nastaví množinu pravidiel bezpečnostnej brány (duplikuje bezpečnostnú bránu) a indikuje, keď bezpečnostnou bránou prejde sieťová premávka, ktorá by mala byť blokovaná. Táto situácia indikuje chybu v konfigurácii bezpečnostnej brány.
  - **Dokumentovanie existujúcich hrozieb v spoločnosti** - IDPS zaznamenáva informácie o hrozbách, ktoré deteguje. Porozumenie frekvencii a charakteru útokom proti výpočtovým zdrojom spoločnosti je užitočné pri identifikácii vhodných bezpečnostných opatrení na ochranu zdrojov spoločnosti. Tieto informácie môžu byť použité na informovanie manažmentu o hrozbách, ktorým spoločnosť čelí.
  - **Odradenie používateľov od porušovania bezpečnostnej politiky** – ak sú používatelia upovedomení o tom, že ich aktivity pri porušovaní bezpečnostnej politiky sú monitorované nástrojmi IDPS, pravdepodobne nebudú porušovať bezpečnostnú politiku, aby neriskovali odhalenie.
- **Základné funkcie IDPS technológií** – existuje veľa typov IDPS technológií, ktoré sa líšia podľa typov rozpoznávaných udalostí a metodológiami, ktoré sú použité na identifikovanie incidentu. Všetky typy IDPS technológií typicky vykonávajú tieto funkcie:
  - **Zaznamenanie informácií majúcich vzťah k sledovanej udalosti** – informácie sú zvyčajne zaznamenané lokálne a môžu byť tiež poslané na centralizovaný logovací server, nástrojom SIEM (Security Information and Event Management) a prípadne podnikovému systému manažmentu.
  - **Informovanie bezpečnostného administrátora o dôležitých sledovaných udalostiach** – toto informovanie sa označuje tiež ako alert (výstraha) a môže byť realizované viacerými spôsobmi. Napríklad e-mailom, správou SMS, správou na používateľský IDPS interfejs, správou SNMP, správou syslog.
  - **Vytváranie správ** – správy sumarizujú monitorované udalosti alebo poskytujú detaily o zvlášť zaujímavých udalostiach.

Princípy detekcie a prevencie prienikov

- **IPS technológie sa líšia od IDS technológií** jednou zásadnou vlastnosťou – IPS technológie **sú schopné reagovať na detegovanú hrozbu** tak, že sa pokúšajú zabrániť, aby bola hrozba úspešná. IPS používajú viaceré techniky reakcie, ktoré je možné rozdeliť do týchto skupín:
  - **IPS zastavuje samotný útok** – príklady realizácie tohto prístupu sú:
    - Ukončenie sieťového spojenia alebo relácie používateľa, ktorá je použitá na útok.
    - Blokovanie prístupu na cieľ (alebo možné ďalšie pravdepodobné ciele) z útočiaceho účtu používateľa, IP adresy alebo iných atribútov útočníka.
    - Blokovanie všetkých prístupov na cielený uzol, službu, aplikáciu alebo ďalší zdroj.
  - **IPS mení bezpečnostné prostredie** - IPS na prerušenie útoku by mohol zmeniť konfiguráciu iných bezpečnostných opatrení. Bežným príkladom je rekonfigurácia sieťového zariadenia (napríklad bezpečnostná brána, smerovač, prepínač) na blokovanie prístupu od útočníka alebo na cieľ a zmenenie hostovej bezpečnostnej brány na cieľ, aby bezpečnostná brána blokovala prichádzajúci útok. Niektoré IPS môžu dokonca spôsobiť aplikáciu záplat na hosta v prípade, že IPS deteguje, že host má slabiny.
  - **IPS mení útočníkov obsah** – niektoré IPS technológie môžu odstrániť alebo zmeniť škodlivú časť útoku a tak útok spravia neškodný. Klasickým príkladom je IPS, ktoré odstráni prílohu s infikovaným súborom v správe elektronickej pošty a až potom umožní, aby „očistený“ email dostal príjemca. Ďalším príkladom je „normalizácia“ prichádzajúcich žiadostí. To znamená, že proxy „prebalí“ obsah žiadosti zničením informácii hlavičky.
- **IDPS technológie** nie sú schopné zabezpečiť úplnú a presnú detekciu.
  - **False positive** – je prípad, keď IDPS nesprávne identifikuje neškodné aktivity ako škodlivé.
  - **False negative** – je prípad, keď IDPS zlyhá pri identifikácii škodlivých aktivít.
  - **Nie je možné eliminovať všetky false positive a false negative.** V mnohých prípadoch pri zmene konfigurácie IDPS na potlačenie false negative sa zvyšuje výskyt false positive. Menenie konfigurácie IDPS s cieľom zlepšenia presnosti detekcie sa nazýva **ladenie** (tuning).
- Väčšina IDPS technológií poskytuje funkcionality na potlačenie techník útočníka, ktoré sa nazývajú **vyhýbanie** (evasion). Vyhýbanie modifikuje formát alebo časovanie škodlivej aktivity (útoku) z hľadiska zmeny vonkajšieho prejavu, ale efekt škodlivej aktivity je ten istý. Napríklad, útočník prekóduje znaky textu špecifickým spôsobom vediac, že cieľ porozumie prekódovaniu a predpokladá, že monitorujúce IDPS prekódovanému textu nerozumie.

Princípy detekcie a prevencie prienikov

- **Štandardné detekčné mechanizmy** – IDPS technológie používajú veľa mechanizmov na detegovanie incidentov. Základné triedy detekčných mechanizmov sú založené na:
  - Príznakoch (signature based)
  - Anomáliách (anomaly based)
  - Analýze stavových protokoloch (stateful protocol analysis)
- **Detekčný mechanizmus založený na príznakoch** – príznak je vzorka, ktorá odpovedá známej hrozbe. Detekcia založená na príznakoch je proces porovnávania príznakov oproti pozorovaným udalostiam s cieľom identifikovať možné incidenty. Príklady príznakov sú:
  - Pokus o spustenie telnetu s loginom „root“, čo je porušenie bezpečnostnej politiky spoločnosti.
  - Správa elektronickej pošty s predmetom „Free pictures“ a s prílohou „freepics.exe“, čo sú charakteristiky známej formy škodlivého kódu
- Ďalšie charakteristiky detekčného mechanizmu založeného na príznakoch:
  - Tento mechanizmus **je veľmi účinný pri detekcii známych hrozieb**, ale neefektívny pri detekcii doteraz neznámych hrozieb (staré hrozby využívajúce mechanizmus vyhýbania)
  - Je to najjednoduchšia metóda, pretože iba porovnáva súčasné jednotky aktivity (paket alebo položku v logu) so zoznamom príznakov použitím operácie porovnania reťazcov.
- **Detekčný mechanizmus založený na anomáliách** – je proces porovnania definovanej normálnej aktivity oproti pozorovaným udalostiam s cieľom identifikovať významné odchýlky:
  - IDPS využívajúce tento mechanizmus detekcie majú uložené profily, ktoré reprezentujú normálne správanie takých objektov ako je používateľ, uzly, sieťové spojenia alebo aplikácie. Profily sú vytvorené monitorovaním charakteristík typickej aktivity za istý čas.
  - IDPS potom používa štatistické metódy na porovnanie súčasných aktivít oproti prahom súvisiacich s profilom. Napríklad detekcia zvýšeného počtu emailových správ oproti očakávanému počtu správ zaznamenanom v profile.
  - Profily môžu byť vytvorené pre mnoho atribútov správania sa ako sú napríklad počty navštívených webových stránok používateľom, počet neúspešných prihlásení sa na uzol, úroveň využitia procesora uzla v danom časovom intervale.

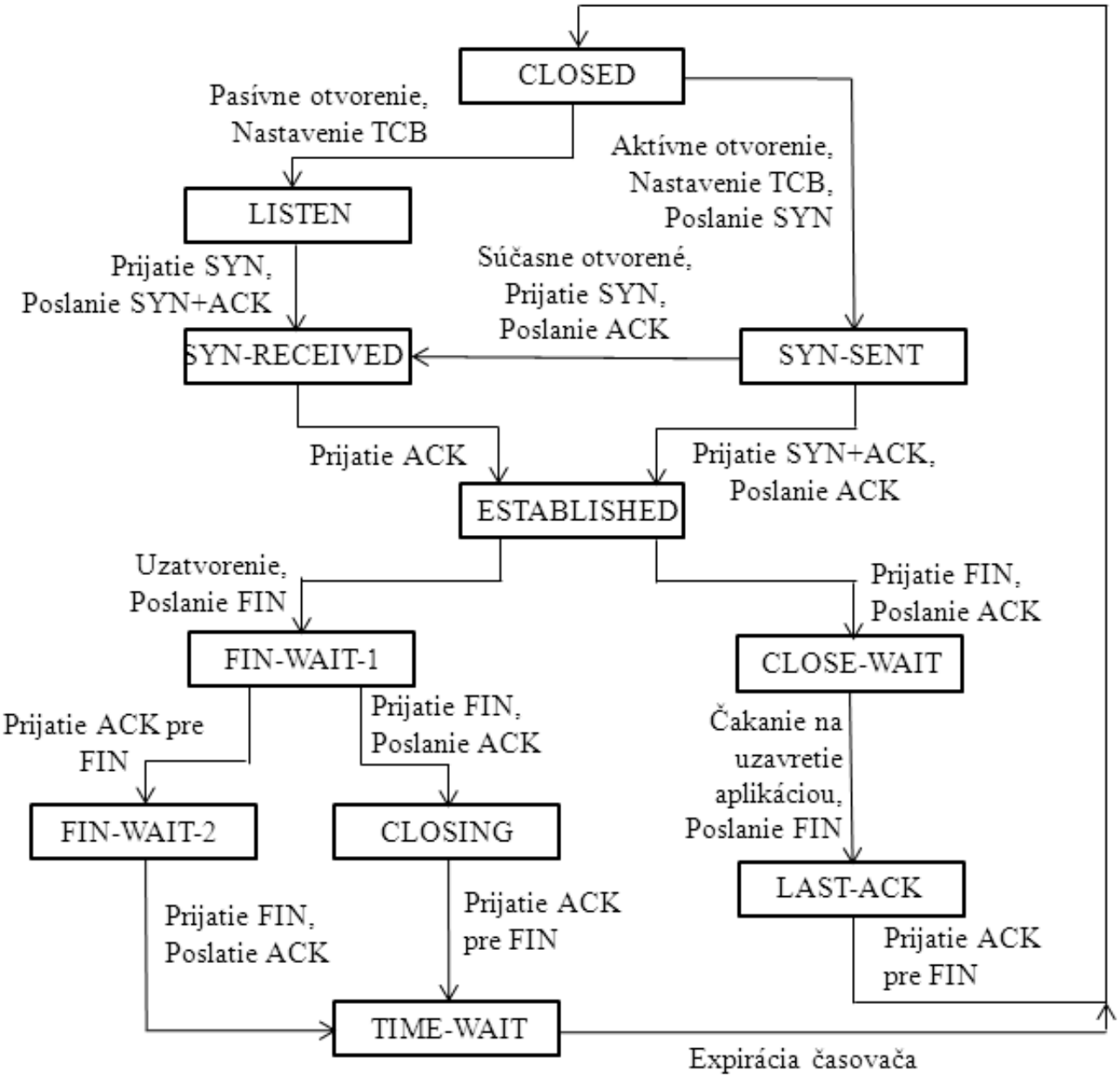
Princípy detekcie a prevencie prienikov

- Ďalšie charakteristiky detekčného mechanizmu založeného na anomáliách:
  - Tento mechanizmus **môže byť veľmi účinný pri detekcii predtým neznámych hrozieb.** Napríklad počítač bol infikovaný neznámym škodlivým kódom, ktorý spotrebováva počítačové zdroje, posiela veľké množstvo emailových správ, inicializuje veľké množstvo sieťových spojení a vykonáva iné aktivity, ktoré sú významne odlišné od zavedeného profilu pre tento počítač.
  - Iniciálny profil je vytvorený v tréningovom intervale v trvaní typicky dní alebo týždňov. Profil detekčného mechanizmu na základe anomálií môžu byť:
    - **Statický** – po vytvorení iniciálneho profilu sa tento profil nemení, pokiaľ IDPS nedostane špecifický príkaz na vytvorenie nového profilu
    - **Dynamický** – je nastavovaný priebežne ako sú zisťované ďalšie udalosti. Tento profil je citlivý na útočníkov, ktorí používajú metódy vyhýbania. Napríklad útočník môže vykonávať príležitostne malé množstvo škodlivých aktivít, čím pomaly zvyšuje frekvenciu a kvantitu škodlivej aktivity v „normálnom“ profile. Takto privedie IDPS k mylnej domnienke, že škodlivé aktivity sú normálne aktivity.
  - **Neúmyselné zahrnutie škodlivých aktivít ako súčasti profilu** je spoločným problémom detekčného mechanizmu anomálií (administrátori ručne modifikujú vytvorený profil tak, že z neho vyhadzujú známe škodlivé aktivity).
  - Pri snahe vytvoriť „presné“ profily, častokrát nastáva situácie, kedy IDPS vytvára veľké množstvo false positive alertov. Je to z toho dôvodu, že zriedka vykonávané neškodlivé aktivity nie sú zahrnuté do profilu, a teda generujú alerty.
- **Detekčný mechanizmus založený na analýze stavových protokolov** – je proces porovnania dopredu určených profilov všeobecne akceptovaných definícií neškodnej aktivity protokolu pre každý stav protokolu oproti sledovaným udalostiam s cieľom identifikovať odchýlky (potenciálne škodlivé stavy).
  - Definícia protokolu je prevzatá zo **štandardizačných dokumentov RFC alebo ich najrozšírenejších implementácií**.
  - Slovo „stavový“ v analýze stavového protokolu znamená, že IDPS je schopný porozumieť a sledovať stav sieťového, transportného alebo aplikačného protokolu, ktoré obsahujú koncept stavu.

Princípy detekcie a prevencie prienikov

- Ďalšie charakteristiky detekčného mechanizmu založeného na analýze stavových protokolov:
  - Tento mechanizmus **môže identifikovať neočakávané postupnosti príkazov** ako je opakované zadanie toho istého príkazu alebo zadanie príkazu bez predchádzajúceho zadanie príkazu, na ktorom je závislý.
  - Tento mechanizmus zvyčajne obsahuje kontroly na **„rozumné“** zadávanie príkazov, napríklad minimálnu a maximálnu dĺžku argumentov prípadne použitú znakovú sadu.
  - Primárnou nevýhodou tohto mechanizmu je jeho **náročnosť na výpočtové zdroje**, pretože pre každý protokol musí vytvoriť novú inštanciu „stavového stroja“ a teda pri viacerých súčasne monitorovaných spojeniach musí pre každé spojenie (a každý použitý stavový protokol) vytvoriť novú inštanciu stavového stroja.
- Na nasledujúcom slajde je obrázok s príkladom stavového stroja pre transportný protokol TCP.

Princípy detekcie a prevencie prienikov



Princípy detekcie a prevencie prienikov

- **Typy technológií IDPS** – existuje veľa typov týchto technológií. Podľa toho aké udalosti monitorujú a spôsobom akým sú nasadzované, možno IDPS technológie rozdeliť do týchto skupín:
  - **Sieťové (network-based)** – monitorujú sieťovú premávku na určitom sieťovom segmente alebo zariadení a analyzujú aktivity sieťových a aplikačných protokolov s cieľom identifikovať podozrivé aktivity. Najčastejšie sú umiestnené na hranici medzi sieťami, v blízkosti hraničných bezpečnostných brán a smerovačov, serverov virtuálnych privátnych sietí (VPN), serverov vzdialeného prístupu a bezdrôtových sietí.
  - **Bezdrôtové (wireless)** – monitorujú premávku bezdrôtovej siete a analyzujú jej bezdrôtové sieťové protokoly s cieľom identifikovať podozrivé aktivity zahrňujúce samotné protokoly. Nie sú schopné identifikovať podozrivé aktivity v protokoloch vyšších úrovní (transportnej a aplikačnej), ktoré bezdrôtová premávka prenáša. Štandardne sa tento typ technológie nasadzuje v rámci bezdrôtovej sieti spoločnosti na jej monitorovanie.
  - **Analýza sieťového správania (network behavior analysis)** – preveruje sieťovú premávku s cieľom identifikovať hrozby generujúce nezvyčajný tok premávky (distribuovaný DoS), určitý typ škodlivého kódu (červy, zadné vrátka) a porušenia politiky. Tento typ technológie sú najčastejšie nasadzované na monitorovanie toku vo vnútornej sieti spoločnosti a niekedy sú nasadzované na miestach, na ktorých monitorujú tok medzi sieťou spoločnosti a externými sieťami (internet, obchodný partner).
  - **Hostové (host-based)** – monitorujú charakteristiky jedného uzla (hosta) a udalosti vyskytujúce sa v rámci tohto uzla s cieľom identifikovať podozrivé aktivity. Príklady monitorovaných aktivít uzla môžu byť sieťová premávka týkajúca sa uzla, systémové logy, bežiace procesy, aktivity aplikácie, prístup k súborom a ich modifikácia a zmeny systémových a aplikačných konfigurácií. Tento typ technológie sa štandardne nasadzuje na kritické uzly ako sú verejne dostupné servery alebo servery obsahujúce citlivé údaje.
- Historicky najstaršie technológie IDPS sú sieťové a niektoré hostové, ktoré sú na trhu už asi 15 rokov. Novším typom IDPS sú na analýzu sieťového správania, ktoré boli primárne vyvinuté na detekciu DDoS útokov a na monitorovanie vnútornej sieti spoločnosti. Bezdrôtové technológie sú nové technológie, ktoré reagujú na hrozby v čoraz populárnejších bezdrôtových lokálnych sieťových technológiách (WLAN).

Technológie IDPS

- **Typické komponenty riešení technológií IDPS sú:**
  - **Senzor alebo agent** – monitorujú alebo analyzujú aktivity. Označenie senzor sa typicky používa pre IDPS, ktoré monitorujú siete. Označenie agent sa typicky používa pre hostové IDPS.
  - **Server manažmentu** – je centralizované zariadenie, ktoré prijíma informácie od senzorov a agentov a spravuje ich. Niektoré servery manažmentu vykonávajú analýzu informácií o udalosti, ktorú poskytli senzory alebo agenti, a sú schopní identifikovať udalosti, ktoré individuálne senzory a agenti schopné nie sú. Párovanie informácií o udalosti z viacerých senzorov alebo agentov (napríklad udalostí spustených z tej istej adresy IP) sa nazýva **korelácia**. Niektoré malé nasadenia technológií IDPS nepoužívajú server manažmentu, ale väčšina nasadení IDPS servery manažmentu používa.
  - **Databázový server** – je úložisko na uloženie informácií, ktoré zaznamenali senzory, agenti a/alebo server manažmentu. Veľa IDPS poskytuje podporu pre databázové servery.
  - **Konzola** – je program, ktorý zabezpečuje **interfejs** medzi IDPS a jeho administrátormi a používateľmi. Typicky je tento program inštalovaný na štandardnom desktope alebo laptope. Niektoré konzoly sú používané iba na administráciu IDPS ako je konfigurácia senzorov alebo agentov, aktualizácia programového vybavenia. Iné konzoly sú používané výlučne iba na monitorovanie a analýzu.
- **Architektúry sietí pre riešenia technológií IDPS** – komponenty IDPS môžu byť prepojené medzi sebou prostredníctvom:
  - **štandardnej sieti spoločnosti (in-band)**. V takomto prípade je vhodné vytvoriť oddelenie siete manažmentu od produkčnej sieti aspoň na úrovni virtuálnej LAN (VLAN). Použitie VLAN zabezpečuje ochranu IDPS komunikácie (ale nie na takej úrovni ako fyzicky oddelenej siete manažmentu), ale ochrana môže zlyhať pri chybnej konfigurácii VLAN alebo pri útoku DoS na produkčnú sieť.
  - **oddelenej sieti (out of band)**, ktorá je výlučne určená pre manažment bezpečnostného softvéru. Tejto oddelenej sieti sa tiež hovorí **sieť manažmentu**.
    - V takomto prípade musí mať senzor alebo agent ďalší **sieťový interfejs** (interfejs manažmentu), ktorým je pripojený do siete manažmentu.
    - Táto architektúra sieti efektívne izoluje sieť manažmentu od produkčnej sieti a **skrýva existenciu a identitu IDPS** pred útočníkmi.
    - Chráni IDPS pred útokmi a zabezpečuje, že IDPS má k dispozícii **dostatočnú sieťovú priepustnosť** aj v prípade útoku DoS na produkčnú sieť.
    - Nevýhodou riešenia sú **dodatočné náklady** na vytvorenie siete manažmentu a **nepohodlie** pre administrátorov IDPS a používateľov IDPS, pretože musia pre svoje činnosti s IDPS používať oddelené počítače.

Technológie IDPS

- **Detekčné schopnosti IDPS technológií** – sú typicky rozsiahle a široké.
  - Väčšina produktov používa kombináciu detekčných techník, ktoré vo všeobecnosti zabezpečujú presnejšiu detekciu a väčšiu flexibilitu pri ladení a prispôsobovaní (customizácii).
  - Väčšina IDPS vyžaduje aspoň nejaké **ladenie a prispôsobovanie** na vylepšenie svojej presnosti detekcie, použiteľnosti a efektívnosti ako je nastavenie vykonania preventívnych akcií v prípade jednotlivých alertov.
  - Vo všeobecnosti platí, že čím sú výkonnejšie ladiace a prispôsobovacích možností IDPS, tým viac môže byť vylepšená presnosť detekcie oproti presnosti prednastavenej konfigurácii.
- Príklady ladiacich a prispôsobovacích možností IDPS technológií:
  - **Prahy (Thresholds)** – sú hodnoty, ktoré nastavujú limity medzi normálnym a abnormálnym správaním. Zvyčajne špecifikujú maximálnu akceptovateľnú úroveň. Prahy sú najviac používané v detekčných mechanizmoch založených na anomáliách a analýze stavových protokolov.
  - **Čierne a biele zoznamy (Blacklists and Whitelists).** Čierny zoznam je zoznam diskrétnych entít ako sú **hosty**, **čísla TCP alebo UDP portov**, **typy a kódy ICMP**, **aplikácií**, **mien používateľov**, **URL**, **mien súborov alebo súborových rozšírení**, ktoré boli v minulosti určené ako súčasť škodlivých aktivít. Niektoré IDPS vytvárajú dynamické čierne zoznamy, ktoré sa využívajú na dočasné blokovanie nedávno detegovaných hrozieb (napríklad aktivity z útočníkovej adresy IP). Biely zoznam je zoznam diskrétnych entít, ktoré sú známe ako neškodné. Zvyčajne sa používajú na báze granularity ako po protokoloch, na redukovanie alebo ignorovanie false positive zahrňujúce známe neškodné aktivity z dôveryhodných hostov. Čierne a biele zoznamy sú najčastejšie používané pri detekčných mechanizmoch na báze príznakov a analýzy stavového protokolu.
  - **Nastavenie alertov.** Niektoré produkty potláčajú alerty v prípade, že útočník v krátkom čase generuje veľa alertov, a dočasne ignorujú všetky črty premávky od útočníka. Toto je ochrana IDPS pred zahltením alertami. Väčšina technológií IDPS dovoľuje administrátorom prispôsobovať každý typ alertu. Príklady akcií, ktoré môžu byť vykonané na type alertu:
    - Preklopenie alertu na zapnutý alebo vypnutý
    - Nastavenie prednastavenej úrovni priority alebo dôležitosti
    - Špecifikovanie informácií, ktoré by mali byť zaznamenané a aká by mala byť použitá notifikačná metóda (napríklad email, instant messaging).

Technológie IDPS

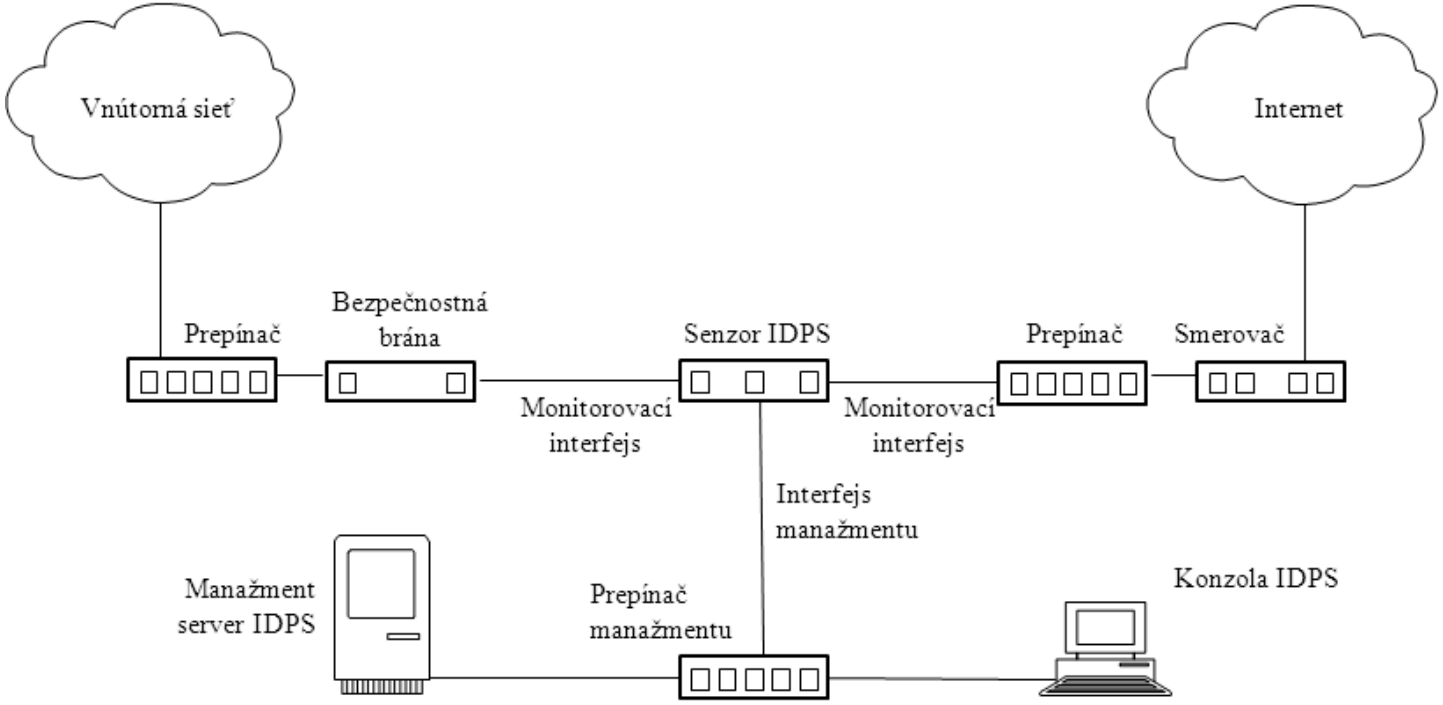
- Príklady ladiacich a prispôsobovacích schopností IDPS technológií:
  - **Prezeranie a editovanie kódu.** – niektoré technológie IDPS dovoľujú administrátorom vidieť časť alebo celý **kód týkajúci sa detekcie**. Zvyčajne to je obmedzené na príznaky, ale niektoré technológie dovoľujú administrátorom vidieť ďalší kód ako sú programy použité na vykonanie analýzy stavových protokolov. Prezretie kódu môže napomôcť analytikom stanoviť, prečo boli generované určité alerty, napomôcť potvrdiť alerty a identifikovať false positive. Schopnosť editovať všetok kód týkajúci sa detekcie a napísať nový kód (napríklad príznaky) je nevyhnutné na plné prispôsobovanie určitých typov detekčných schopností. Samozrejme, editovanie kódu vyžaduje programovacie zručnosti a zručnosti v detekcii prienikov. Navyše niektoré technológie IDPS používajú proprietárne programovacie jazyky. Chyby zavedené do kódu počas procesu prispôsobovania môžu spôsobiť **nesprávnu činnosť IDPS** alebo jej zlyhanie, preto by mali administrátori narábať s prispôsobovaním rovnako obozretne ako pri každej inej zmene produkčného systémového kódu.

Sieťové IDPS

- **Komponenty a architektúra** – sú uvedené hlavné komponenty typickej sieťovej technológie IDPS a najbežnejšie sieťové architektúry s týmito komponentmi.
- **Typické komponenty** – predstavujú **senzory**, jeden alebo viacero **serverov manažmentu**, viacero **konzolí** a voliteľne jeden alebo viacero **databázových serverov** (pokiaľ sieťové IDPS podporuje ich používanie). Sieťové senzory IDPS monitorujú a analyzujú sieťové aktivity na jednom alebo viacerých sieťových segmentoch. Sieťové interfejsové karty (NIC) zabezpečujúce monitorovanie pracujú v promiskuitnom režime (akceptujú všetky prichádzajúce pakety bez ohľadu na ich cieľovú adresu). Väčšina nasadení IDPS používa viacero senzorov (veľké nasadenia IDPS aj stovky senzorov). Senzory sieťových IDPS sú dostupné v dvoch prevedeniach:
  - **Zariadenie.** V tomto prevedení senzor pozostáva zo špecializovaného hardvéru a softvéru. Hardvér je optimalizovaný na použitie senzora vrátane špecializovanej karty NIC a jej ovládača na efektívne odchytávanie paketov a špecializovaných procesorov alebo ďalších hardvérových komponentov podporujúcich analýzu. Časť alebo celý softvér môže byť z dôvodu zvýšenia efektívnosti umiestnený vo firmvéri. Tieto zariadenia často obsahujú prispôsobený, utesnený operačný systém, ku ktorému sa nepredpokladá prístup administrátorov. Príklady: rad CISCO IDS 4200, IBM Real Secure Network
  - **Iba softvér.** Niektorí predajcovia predávajú senzorový softvér bez zariadenia. Administrátori inštalujú tento softvér na počítače, ktoré splňujú určité špecifikácie. Senzorový softvér môže obsahovať prispôsobený (customized) operačný systém alebo senzorový softvér môže byť inštalovaný štandardnom operačnom systéme ako iná aplikácia. Príklady: Snort, Bro
- **Architektúry sieti a umiestnenie senzorov** – v prípade nasadenia sieťových technológií IDPS sa odporúča **vytvorenie sieti manažmentu**. Ak sa nasadia prostriedky IDPS bez sieti manažmentu, potom je vhodné na ochranu komunikácie medzi prvkami technológie IDPS použiť virtuálnu LAN (VLAN). Senzory môžu byť nasadené v dvoch režimoch:
  - **Prechodový senzor (Inline)** – všetka monitorovaná premávka prechádza senzorom (podobne ako všetka premávka prechádza bezpečnostnou bránou). Má **dva sieťové interfejsy** na monitorovanie premávky siete (cez tieto interfejsy prechádza sieťová premávka) a **jeden interfejs manažmentu** na pripojenie do siete manažmentu.
  - **Pasívny senzor** – monitoruje kópiu skutočnej sieťovej premávky. Žiadna premávka neprechádza senzorom.

Sieťové IDPS

- **Charakteristika architektúr s prechodovými senzormi sieťových IDPS**
  - V skutočnosti sú niektoré prechodové senzory **hybridy bezpečnostná brána / IDPS zariadenie**.
  - Primárnym dôvodom pre nasadenie prechodových senzorov IDPS je skutočnosť, aby boli schopné **zastaviť útok blokovaním sieťovej premávky**.
  - Prechodové senzory sú typicky umiestnené na tie miesta v sieti, kde sú umiestňované bezpečnostné brány a iné sieťové bezpečnostné zariadenia a to na hranici medzi sieťami, na pripojení do externých sietí a hranicami medzi rozdielnymi vnútornými sieťami, ktoré by mali byť oddelené.
  - Prechodové senzory, ktoré nie sú hybridy bezpečnostná brána / IDPS zariadenie sú často umiestňované **na bezpečnejšiu stranu siete** (z tej strany hranice, kde je sieť bezpečnejšia), aby spracovávali menší objem premávky. Senzory môžu byť tiež umiestnené **na menej bezpečnej strane sieti**, aby zabezpečovali ochranu redukovaním záťaže oddeľovacieho zariadenia ako je bezpečnostná brána. Na nasledujúcom obrázku je príklad takejto architektúry.

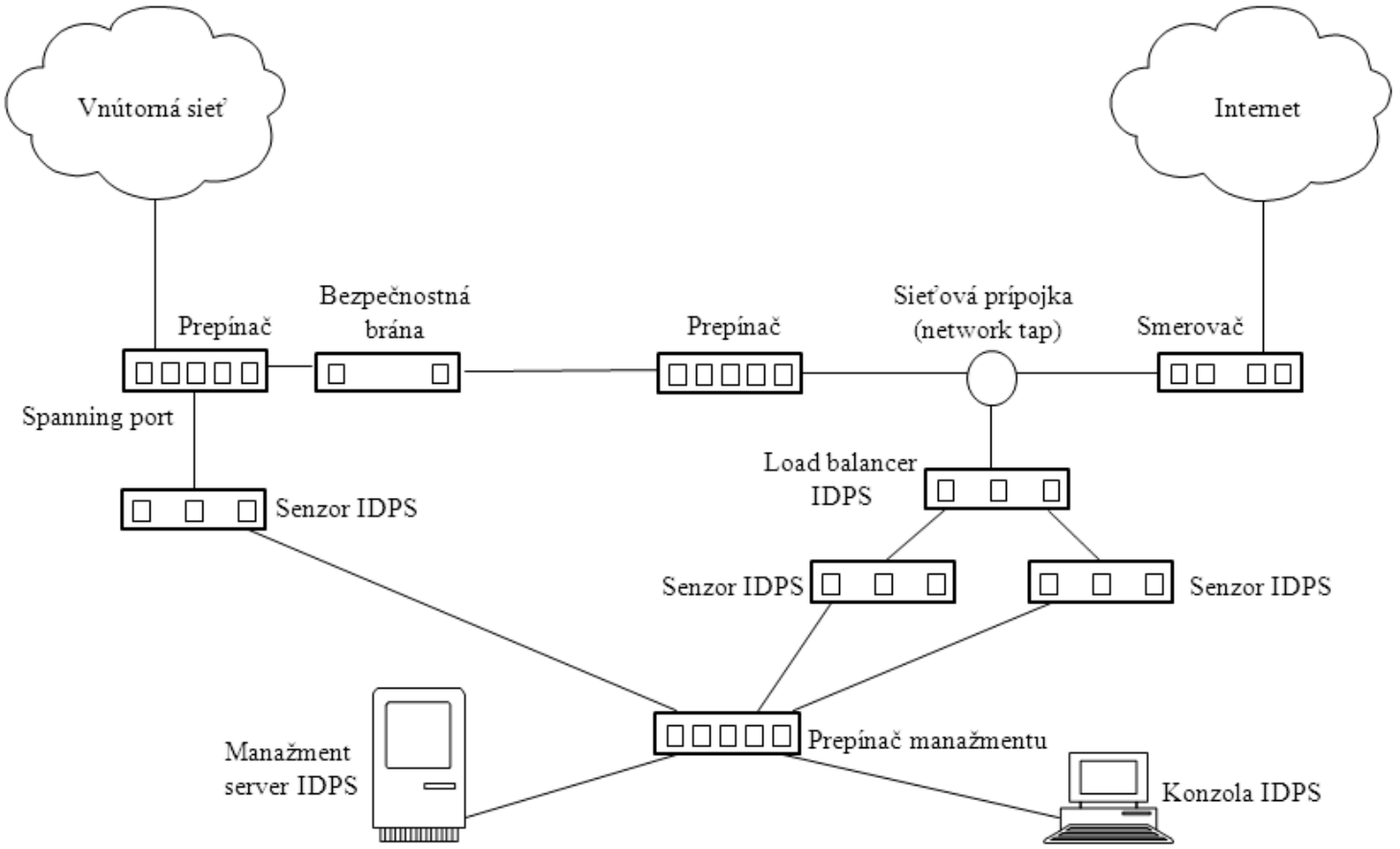


Sieťové IDPS

- **Charakteristika architektúr s pasívnymi senzormi sieťových IDPS** – pasívne senzory sú typicky nasadzované tak, aby monitorovali kľúčové sieťové miesta ako sú hranice medzi sieťami, kľúčové sieťové segmenty ako sú aktivity v demilitarizovanej zóne (DMZ). Pasívne senzory môžu monitorovať premávku prostredníctvom rôznych metód, ako napríklad:
  - **Pokrývajúci port (spanning port)** - je port prepínača, ktorý je schopný vidieť **všetku sieťovú premávku prechádzajúcu cez prepínač**. Pripojením senzora na pokrývajúci port môže senzor monitorovať premávku na / z veľa uzlov. Táto metóda monitorovania je relatívne ľahká a lacná, môže byť tiež ale aj problematická. Ak prepínač **nie je správne nakonfigurovaný**, potom pokrývajúci port nemusí vidieť všetku premávku. Ďalším problémom s pokrývajúcimi portami je možnosť, **že prepínač je preťažený** a pokrývajúci port nemusí byť schopný vidieť všetku premávku, prípadne pokrývajúci port môže byť dočasne zablokovaný. Tiež veľa prepínačov **majú iba jeden pokrývajúci port** a často krát je potreba mať viacero technológií, ako sú nástroje na monitorovanie siete, nástroje na forenznú analýzu siete a pre ďalšie IDPS senzory, ktoré monitorujú tú istú premávku.
  - **Sieťová prípojka (network tap)** – je priame prepojenie medzi senzorom a samotným fyzickým médiom ako je napríklad optické vlákno. Prípojka dodáva senzoru kópiu celej sieťovej premávky, ktorá sa prenáša cez médium. Prípojka funguje podobne ako pokrývajúci port s tým rozdielom, že prepínače sú vo výrobe vybavené pokrývajúcim portom a prípojku treba zaobstarať a inštalovať.
  - **Vyvažovač záťaže IDS (load balancer IDS)** – je zariadenie, ktoré **dáva dokopy a smeruje premávku** siete do monitorovacích systémov vrátane IDPS senzorov. Vyvažovač dostane kópiu sieťovej premávky z jedného alebo viacerých pokrývajúcich portov alebo sieťových prípojok a dáva dokopy premávku z rôznych sietí (napríklad znovu skladá reláciu, ktorá bola rozdelená medzi dve siete). Potom vyvažovač, na základe pravidiel nastavených administrátorom, posiela kópie premávky jednému alebo viacerým prijímajúcim zariadeniam vrátane senzorov IDPS. Pravidlá definujú vyvažovačovi aký typ premávky pošle akému prijímaciemu zariadeniu. Bežné konfigurácie vyvažovača obsahujú takéto možnosti:
    - **Poslať všetku premávku viacerým IDPS senzorom** – táto možnosť podporuje vysokú dostupnosť alebo viacero typov IDPS vykonáva paralelnú analýzu tej istej aktivity
    - **Dynamicky rozdeliť premávky medzi viacero senzorov podľa objemu** – táto možnosť predstavuje typické rozkladanie záťaže, čo znamená, že žiadny senzor nie je zahltený množstvom premávky a príslušnou analýzou
    - **Rozdeliť premávku** na základe adresy IP, protokolov alebo iných charakteristík medzi viacero senzorov IDPS. Táto možnosť môže byť realizovaná z dôvodov rozloženia záťaže ako napríklad v prípade, keď jeden senzor je venovaný webovým aktivitám a ďalší senzor IDPS monitoruje všetky ostatné aktivity. Rozdelenie premávky môže byť tiež s cieľom detailnejšej analýzy určitých typov premávky. Treba si ale uvedomiť, že rozdelenie premávky medzi viacero senzorov môže spôsobiť zníženie presnosti detekcie (súvisiace udalosti sú rozdelené).

Sieťové IDPS

Príklad architektúry pasívneho senzora sieťového IDPS



- Viacero techník so senzorom na prevenciu prienikov **vyžaduje nasadenie senzora v prechodovom režime a nie v pasívnom režime**. Pretože pasívne techniky monitorujú kópiu premávky, typicky neposkytujú spoľahlivý spôsob pre senzor, aby zastavil premávku od dosiahnutia jej cieľa. V niektorých prípadoch môže pasívny senzor vyslať na sieť paket a pokúsiť sa prerušiť kritické spojenie, ale takéto metódy sú vo všeobecnosti menej efektívne, ako metódy používané prechodovými senzormi.

Sieťové IDPS

- **Bezpečnostné možnosti** – sieťové IDPS poskytujú široké možnosti bezpečnostných schopností, ktoré môžu byť štruktúrované do štyroch kategórií: zhromaždenie informácií, zaznamenanie, detekcia a prevencia.
- **Možnosti zhromaždenia informácií** – niektoré sieťové IDPS ponúkajú obmedzené schopnosti zhromažďovania informácií, čo znamená, že zbierajú informácie o uzloch a sieťových aktivitách zahrňujúcich tieto uzly. Príklady možností zhromažďovania informácií sú:
  - **Identifikovanie uzlov.** Senzor IDPS môže byť schopný vytvoriť zoznam uzlov pripojených do siete spoločnosti podľa adries IP alebo adries MAC. Tento zoznam môže byť použitý ako **profil na identifikáciu nových uzlov na sieti**.
  - **Identifikovanie operačných systémov.** Senzor IDPS môže byť schopný rôznymi technikami identifikovať operačné systémy a ich verzie, ktoré sa používajú v spoločnosti. Napríklad, senzor môže sledovať, ktoré **porty sa používajú na každom uzle**, čo môže indikovať určitý operačný systém (Windows, Unix). Ďalšou technikou je **analyzovanie hlavičiek paketov** na určité nezvyčajné charakteristiky alebo kombinácie charakteristík, ktorými sa prejavujú určité operačné systémy. Tomuto sa hovorí **pasívne zistenie odtlačku** (passive fingerprinting).
  - **Identifikovanie aplikácií.** Pre niektoré aplikácie môže senzor IDPS identifikovať používanú verziu aplikácie tak, že sleduje, ktoré porty sú používané a monitoruje určité charakteristiky komunikácie aplikácie. Napríklad, keď klient zriadi spojenie so serverom, potom server môže oznámiť klientovi aká softvérová verzia aplikačného servera je vykonávaná a naopak.
  - **Identifikovanie sieťových charakteristík.** Niektoré senzory IDPS zbierajú všeobecné informácie o sieťovej premávke majúcej vzťah ku konfigurácii sieťových zariadení a uzlov, také ako sú informácie o **počte hopov nedzi dvomi zariadeniami**. Táto informácia môže byť použitá na detekciu zmien v sieťovej konfigurácii.
- **Možnosti zaznamenania** – sieťové IDPS typicky vykonávajú rozsiahle zaznamenanie údajov majúcich vzťah k detegovanej udalosti. Tieto údaje môžu byť použité na **potvrdenie platnosti alertu, na vyšetrenie incidentov a na koreláciu udalostí medzi IDPS a ostatnými logovacími zdrojmi**. Väčšina sieťových IDPS je schopná vykonať zachytenie paketov. Štandardne sa to vykonáva vtedy, keď sa generuje alert. Zachytávajú sa alebo následné aktivity v spojení po alerte alebo sa zanamená celé spojenia (ak IDPS dočasne uchovával predchádzajúce pakety).

Sieťové IDPS

- **Možnosti zaznamenania** – záznam sieťového IDPS môže vo všeobecnosti obsahovať tieto údajové polia (položky):
  - Časová pečiatka (dátum a čas)
  - ID spojenia alebo relácie (typicky postupné alebo jedinečné číslo priradené každému TCP spojeniu alebo podobným skupinám paketov pre protokoly bez spojenia)
  - Typ udalosti alebo alertu
  - Rating (napríklad priorita, dôležitosť, dopad, dôvernosť)
  - Protokol sieťovej, transportnej a aplikačnej vrstvy
  - Zdrojová a cieľová adresa IP
  - Zdrojový a cieľový port TCP alebo UDP, alebo typy ICMP a kódy
  - Počet slabík prenesených týmto spojením
  - Dekódované údaje užitočného nákladu (payload), ako sú žiadosti a odpovede aplikácie
  - Informácie viažúce sa na stav (napríklad autentizované meno používateľa)
  - Vykonané preventívne akcie (ak treba).
- **Možnosti detekcie** – sieťové IDPS typicky ponúkajú široké a všeobecné detekčné schopnosti. Väčšina produktov využíva **kombináciu mechanizmov detekcie pomocou príznakov, anomálií a analýzy stavových protokolov** (in-depth analysis bežných protokolov). Detekčné mechanizmy sú zvyčajne pevne previazané, napríklad stroj na detekciu mechanizmu analýzy stavových protokolov môže rozobrať aktivity do žiadostí a odpovedí, pričom každá z nich je preverovaná na anomálie a porovnaná s príznakom známych škodlivých aktivít. Detekčné schopnosti možno analyzovať z týchto pohľadov: typy detegovaných udalostí, presnosť detekcie, ladenie a prispôsobenie, obmedzenia technológie.

Sieťové IDPS

- **Typy detegovaných udalostí** – najbežnejšie typy detegovaných udalostí senzormi sieťových IDPS sú:
  - **Prieskum a útoky na aplikačnej vrstve.** Napríklad odchytenie bannera, pretečenie vyrovnávacej pamäti, útoky na formátové reťazce, hádanie hesla, prenášanie škodlivého kódu. Väčšina sieťových IDPS analyzuje temer všetky najrozšírenejšie aplikačné protokoly, takisto ako databázové protokoly, aplikácie instant messaging a softvér na peer-to-peer zdieľanie súborov.
  - **Prieskum a útoky na transportnej vrstve.** Napríklad skenovanie portov, nezvyčajná fragmentácia paketov, záplava SYN. Najfrekventovanejšie analyzované protokoly transportnej vrstvy sú TCP a UDP.
  - **Prieskum a útoky na sieťovej vrstve.** Napríklad falošná (spoofed) adresa IP, nedovolená hodnota hlavičky IP. Najfrekventovanejšie analyzované protokoly sieťovej vrstvy sú IPv4, ICMP a IGMP. Možnosť analýzy protokolu IPv6 sa medzi produktmi výrazne líši. Niektoré produkty sú schopné spracovať premávku IPv6 a tunelovaného IPv6 ako je zaznamenanie zdrojovej a cieľovej adresy IP a vybrať prenášané údaje (payload) (napríklad HTTP, SMTP) na hĺbkovú analýzu (in-depth analysis). Iné produkty sú schopné vykonať plnú analýzu protokolu IPv6, takú ako je potvrdenie platnosti výberu volieb v IPv6, identifikácia anomálneho použitia protokolu.
  - **Neočakávané aplikačné služby.** Napríklad tunelované protokoly, zadné vrátka, uzly vykonávajúce neautorizované aplikačné služby. Tieto prípady sú detegované prostredníctvom mechanizmu analýzy stavového protokolu, ktorý môže určiť či aktivity v spojení sú konzistentné s očakávanými aktivitami aplikačného protokolu, alebo prostredníctvom mechanizmu detekcie anomálií, ktoré sú schopné identifikovať zmeny v sieťových tokoch a otvoriť porty na uzloch.
  - **Porušenie politiky.** Napríklad použitie nevhodných webových sídiel, použitie zakázaných aplikačných protokolov. Niektoré typy porušení bezpečnostnej politiky môžu byť detegované pomocou IDPS, ktoré potom umožňujú administrátorovi špecifikovať charakteristiky nedovolenej aktivity ako čísla portov TCP a UDP, adresy IP, mená webových sídiel a iné súčasti údajov zistené preskúmaním sieťovej premávky.
- **Typy detegovaných udalostí** – niektoré IDPS sú schopné monitorovať vykonávanie **iniciálneho dojednávania šifrovacích nástrojov** a identifikovať softvér klienta alebo servera, ktorý má známe slabiny alebo je chybne konfigurovaný. Tento prípad môže zahrňovať protokoly aplikačnej vrstvy ako je SSH (Secure SHell) a SSL (Secure Socket Layer) a virtuálna privátna sieť VPN na sieťovej vrstve vytvorená protokolom IPSec.

Sieťové IDPS

- **Možnosti prevencie** – iba pasívne senzory sieťových IDPS:
  - **Ukončenie aktuálneho TCP spojenia.** Pasívny senzor IDPS môže skúsiť ukončiť existujúcu reláciu TCP tak, že pošle pakety **TCP reset** obidvom komunikujúcim koncom. Tejto technike sa hovorí **odstrelenie relácie** (session sniping). Senzor to urobí tak, že pre oba komunikujúce konce to vyzerá tak, že ten druhý koniec chce ukončiť spojenie. Cieľom je, aby jeden komunikujúci koniec ukončil spojenie ešte predtým ako by útok bol úspešný. Bohužiaľ istým problémom je to, že v mnohých prípadoch **pakety TCP reset nie sú prijaté načas** z dôvodov časového oneskorenia potrebného na monitorovanie a analyzovanie premávky, detekcie útoku a poslatie paketov cez sieť komunikujúcim koncom. Táto technika je aplikovateľná iba na TCP a nemôže byť aplikovateľná napríklad na UDP a ICMP. Technika odstrelenia relácie nie je v súčasnosti široko používaná, pretože iné prevenčné schopnosti sú efektívnejšie
- **Možnosti prevencie** – iba prechodové senzory sieťových IDPS:
  - **Vykonanie prechodového firewallingu.** Väčšina senzorov IDPS ponúka schopnosti bezpečnostnej brány (firewall), ktoré môžu byť použité na zastavenie alebo odmietnutie podozrivej sieťovej aktivity
  - **Obmedzenie na použitie prenosového pásma**. V prípade, že určitý protokol sa používa nevhodne, ako napríklad na útok DoS, distribúciu škodlivého kódu alebo peer-to-peer zdieľanie súborov, niektoré prechodové senzory IDPS môžu **obmedziť percento sieťového prenosového pásma**, ktoré tento protokol používa. Toto opatrenie zabraňuje aktivitám negatívne dopadajúcim na používanie prenosového pásma pre iné zdroje.
  - **Zmena škodlivého obsahu.** Niektoré prechodové senzory IDPS môžu **sanovať časť paketu**, čo znamená, že je nahradený škodlivý obsah za neškodný obsah a sanovaný paket je odoslaný do svojho cieľa. Senzor, ktorý funguje ako proxy by mohol vykonať automatickú normalizáciu premávky, ako prebalenie aplikačných údajov do nových paketov. Toto má efekt sanovania niektorých útokov zahrňujúcich paketové hlavičky a niektoré aplikačné hlavičky bez ohľadu na to, či IDPS detegoval útok alebo nie. Niektoré senzory sú schopné tiež oddeliť infikované prílohy z emailových správ a odstrániť ďalšie nesúvisiace časti škodlivého obsahu zo sieťovej premávky.

Sieťové IDPS

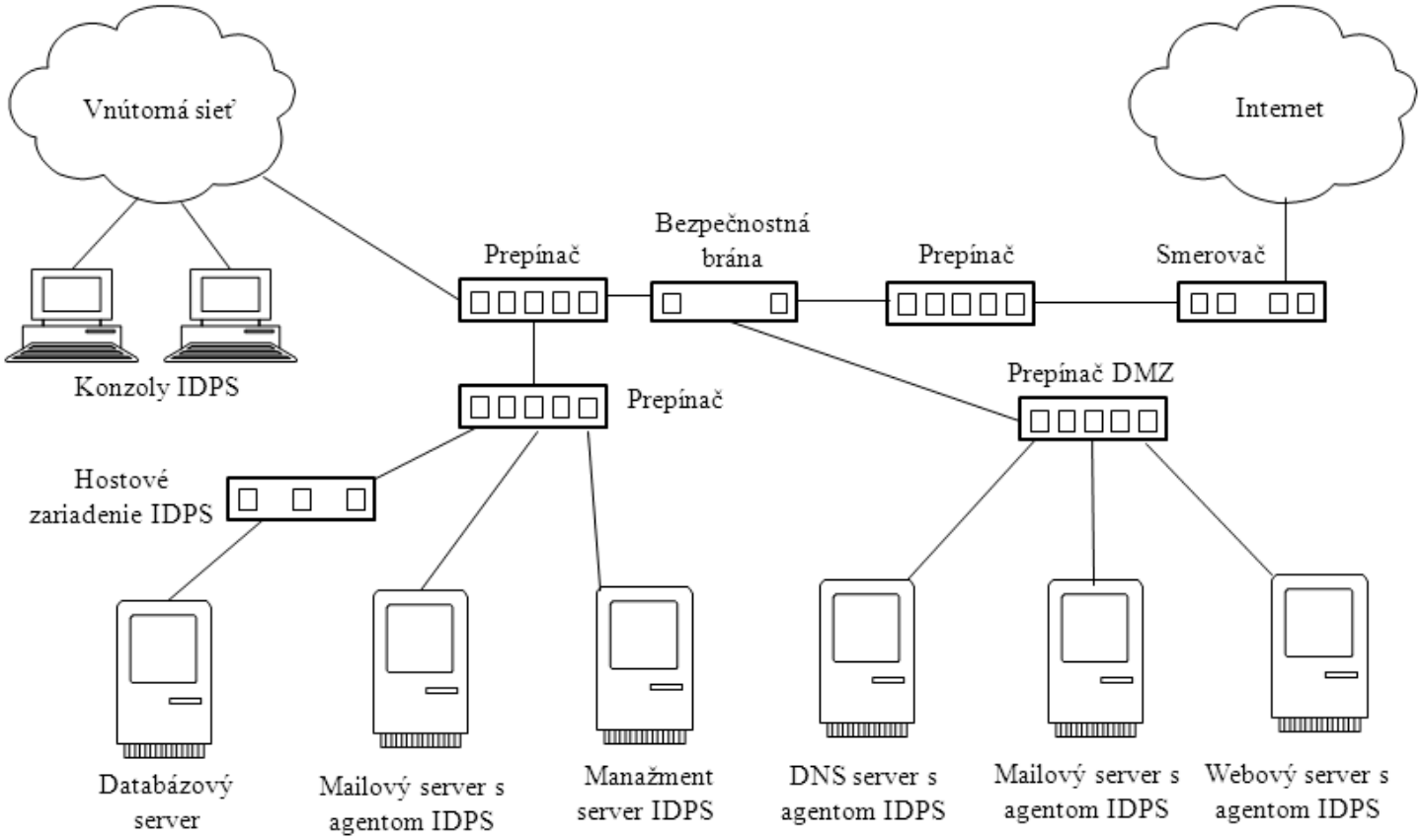
- **Možnosti prevencie** – aj pasívne aj prechodové senzory sieťových IDPS:
  - **Rekonfigurácia iných sieťových bezpečnostných zariadení.** Veľa senzorov IDPS môže dať pokyn sieťovým bezpečnostným zariadeniam ako sú bezpečnostné brány, smerovače a prepínače **na ich rekonfiguráciu s cieľom blokovania určitého typu aktivity alebo ich smerovania inam**. Toto môže byť nápomocné v niekoľkých situáciách ako je držanie externého útočníka mimo siete a danie do karantény interný uzol, ktorý bol kompromitovaný (napríklad premiestniť ho do karanténnej VLAN). Tieto preventívne techniky sú užitočné iba pre sieťovú premávku, ktorá môže byť vyčlenená podľa charakteristiky hlavičky paketu (napríklad adresy IP a čísla portov) a typicky rozpoznaná sieťovými bezpečnostnými zariadeniami.
  - **Vykonávanie programov tretích strán alebo skriptov.** Niektoré senzory IDPS sú schopné, v prípade detekcie určitej škodlivej aktivity, **vykonať administrátorom určený skript alebo program**. Toto môže spustiť ľubovoľnú preventívnu akciu požadovanú administrátorom ako je rekonfigurácia iných bezpečnostných zariadení s cieľom blokovať škodlivé aktivity. Programy tretích strán alebo skripty sú častejšie používané v prípade, že IDPS nepodporuje také preventívne akcie, čo by vyžadovali administrátori.
- **Možnosti prevencie** – väčšina senzorov IDPS dovoľuje administrátorom **špecifikovať prevencie schopné konfigurácie pre každý typ alertu**. Toto zvyčajne zahrňuje povolenie alebo zakázanie prevencie, rovnako ako špecifikovanie ktoré prevenčné možnosti by mali byť použité. Niektoré senzory IDPS majú režim učenia alebo simulácie, ktorý potláča všetky preventívne akcie a namiesto toho indikuje kedy by bola preventívna akcia vykonaná. Tento režim umožňuje administrátorom monitorovať a jemne ladiť preventívne schopnosti konfigurácie predtým než sa povolia, čo redukuje riziko náhleho blokovania neškodnej aktivity.

Hostové IDPS

- **Monitorujú charakteristiky jedného hosta a udalosti vyskytujúce sa v tomto hoste na podozrivé aktivity.** Príklady monitorovaných typov charakteristík hostovým IDPS je bezdrôtová a drôtová sieťová premávka (týkajúca sa iba tohto hosta), systémové logy, prístup k a modifikácia súborov a zmeny konfigurácií systému alebo aplikácií.
- **Typické komponenty** – Väčšina hostových IDPS majú detekčné softvér označovaný ako **agent,** ktorý je nainštalovaný na danom hoste. Agent monitoruje aktivitu na danom hoste a pokiaľ sú povolené funkcie IDPS, potom vykonáva aj prevenčné aktivity. Agenti posielajú údaje na **servery manažmentu**, ktoré môžu voliteľne využiť databázové servery na uloženie údajov. **Konzoly** sa používajú na manažment a monitorovanie.
  - Niektoré produkty hostových IDPS používajú **špecializované zariadenia** vykonávajúce softvér agenta namiesto inštalácie softvérového agenta na jednotlivého hosta. Zariadenie je umiestnené na monitorovanie sieťovej premávky vstupujúcej a odchádzajúcej z určitého hosta. Technicky by tieto zariadenia mohli považovať za sieťové IDPS, pretože sú nasadené ako prechodové na monitorovanie sieťovej premávky. Avšak zvyčajne sledujú aktivity len pre jeden konkrétny typ aplikácie, takú ako je webový server alebo databázový server. To znamená, že sú viac špecializované než štandardné sieťové IDPS. Takisto bežiaci softvér na zariadení má často rovnaké alebo podobné funkcie ako hostoví agenti.
- Každý agent je typicky určený na ochranu jedného z nasledujúcich:
  - **Server -** okrem minitorovania operačného systému servera môže agent monitorovať niektoré bežné aplikácie.
  - **Klientsky host (desktop alebo notebook)** - agenti určení na monitorovanie používateľských hostov, zvyčajne monitorujú operačný systém a bežné klientske aplikácie ako sú klienti emailu alebo webové prehliadače.
  - **Aplikačné služby** - niektorí agenti vykonávajú monitorovanie iba špecifickej aplikačnej služby ako program webového servera alebo program databázového servera. Tento typ agenta je tiež známy ako **aplikačný IDPS**.
- Väčšina produktov nemá agentov pre ďalšie typy hostov ako sú sieťové zariadenia (bezpečnostné brány, smerovače, prepínače).

Hostové IDPS

Príklad architektúry rozloženia hostových agentov IDPS



- **Architektúry sietí** – pre hostové IDPS sú zvyčajne veľmi jednoduché. Vzhľadom k tomu, že agenti sú nasadení na existujúce hosty v sieti spoločnosti, komponenty obvykle komunikujú prostredníctvom týchto sietí (produkčných sietí) namiesto použitia oddelenej siete manažmentu. Väčšina produktov šifruje svoju komunikáciu, bráni v útočníkom v odpočúvaní citlivých informácií. Agenti - zariadenia sú typicky umiestnení v prechodovom zapojení bezprostredne pred hostom, ktorého chránia (viď obrázok).

Hostové IDPS

- **Umiestnenie agentov** – v štruktúre siete spoločnosti sa agenti umiestňujú:
  - Agenti hostových IDPS sú najčastejšie nasadené **na kritické hosty**, ako sú verejne dostupné servery a servery, ktoré obsahujú citlivé informácie.
  - Niekedy sa používajú agenti hostových IDPS predovšetkým na analýzu aktivít, ktoré **nemôžu byť monitorované inými bezpečnostnými opatreniami**. Napríklad senzory sieťových IDPS nemôžu analyzovať aktivity v šifrovanej komunikácii po sieti, ale agenti hostových IDPS inštalované na koncových bodov môžu vidieť nezašifrovanú aktivitu.
- **Architektúry hostov** – možno rozdeliť podľa toho, do akej miery modifikujú prostredie hosta, na ktorom sú nasadené.
  - Pre zabezpečenie možnosti prevencie narušenia, väčšina agentov IDPS **mení interné architektúru hostov**, na ktorých sú nainštalovaní. Realizuje sa to zvyčajne pomocou **podložky (shim)**, čo je vrstva kódu umiestneného medzi existujúce vrstvy kódu. Podložka zachytáva údaje na mieste, kde by boli normálne odovzdané z jednej časti kódu do druhej časti kódu. Podložka môže potom analyzovať údaje a zistiť, či by **údaje mali byť prenesené alebo odmietnuté**. Agenti hostových IDPS môžu používať podložky pre niekoľko typov zdrojov vrátane sieťovej premávky, aktivity súborového systému, systémových volaní, aktivity Windows Registry a bežných aplikácií (napr. e-mail, web).
  - Niektorí agenti hostových IDPS **nemenia architektúru hostiteľa** a monitorujú aktivitu bez podložiek alebo analyzujú prejavy činnosti, ako sú položky v záznamoch a modifikácie súborov. Aj keď je tento prístup pre hosta menej rušivý, znižuje možnosť IDPS zasahovať do normálnej prevádzky hosta. Tieto metódy sú tiež všeobecne menej účinné pri odhaľovaní hrozieb a často nie je možné vykonávať žiadne preventívne opatrenia.
- **Bezpečnostné možnosti** – hostové IDPS poskytujú široké možnosti bezpečnostných možností, ktoré môžu byť štruktúrované do štyroch kategórií: zaznamenanie, detekcia, prevencia a ďalšie.

Hostové IDPS

- **Možnosti zaznamenania** – hostové IDPS typicky vykonávajú rozsiahle zaznamenanie údajov majúcich vzťah k detegovaným udalostiam. Tieto údaje môžu byť použité na **potvrdenie platnosti alertu, na vyšetrenie incidentov a na koreláciu udalostí medzi hostovými IDPS a ostatnými logovacími zdrojmi**. Údajové polia bežne zaznamenané hostovým IDPS obsahujú tieto informácie:
  - Časová pečiatka (dátum a čas)
  - Typ udalosti alebo alertu
  - Rating (napríklad priorita, dôležitosť, dopad, dôvernosť)
  - Detaily udalosti špecifické typu udalosti ako napríklad informácia o adrese IP a čísle portu, informácie o aplikácii, menách súborov a cestách a používateľovom ID
  - Vykonané preventívne akcie (ak nejaké boli)
- **Možnosti detekcie** – väčšina hostových IDPS majú schopnosť detegovať niekoľko typov škodlivých aktivít. Často používajú kombináciu **mechanizmu príznaku na identifikáciu známych útokov s mechanizmom anomálií a s politikami alebo sadami pravidiel na identifikáciu doposiaľ neznámych útokov**. Detekčné možnosti hostových IDPS sú ovplyvnené týmito faktormi: typy detegovaných udalostí, presnosť detekcie, ladenie a prispôsobovanie a obmedzenie technológie.
- **Typy detegovaných udalostí** hostových IDPS sa významne menia v závislosti na použitých detekčných mechanizmoch. Špecifické techniky bežne používané v hostových IDPS obsahujú tieto:
  - **Analýza kódu.** Agenti môžu používať jednu alebo viacero z nižšie uvedených techník na identifikáciu škodlivej činnosti na základe analýzy pokusov o vykonanie kódu. Všetky tieto techniky sú užitočné pri zastavení škodlivého softvéru a môžu tiež zabrániť ďalším útokom, ktoré by umožnili neoprávnenému prístupu, spúšťaniu kódu alebo zvyšovaniu privilégií.
    - **Analýza správania kódu.** Predtým než kód pobeží normálne na hostovi, **môže byť najprv vykonaný vo virtuálnom prostredí** (sandbox – pieskovisko) s cieľom analýzy jeho správania sa a porovnania oproti profilom alebo pravidlám dobrého alebo zlého správania sa (získanie administrátorských privilégií alebo prepísanie systémového kódu).
    - **Detekcia pretečenia vyrovnávajúcej pamäti.** Pokusy vykonať pretečenie zásobníka alebo voľnej zreťazenej pamäti (heap) možno zistiť hľadaním ich typických vlastnosti, ako sú **určité sekvencie inštrukcií a pokusy o prístup do iných častí pamäte než ktorá je pridelená procesu**.

Hostové IDPS

- **Monitorovanie systémového volania.** Agent vie, **ktoré aplikácie a procesy by mali byť volajúce ktoré iné aplikácie a procesy alebo vykonávajúce určité akcie**. Napríklad agent môže rozpoznať proces pokúšajúci sa odchytiť stláčanie kláves ako je napríklad keylogger. Agenti môžu tiež obmedziť, ktoré ovládače môžu byť zavedené, čo môže zabrániť inštalácii rootkitu a iným útokom.
- **Zoznamy aplikácií a knižníc.** Agent by mohol monitorovať každú aplikáciu a knižnicu (napr., dynamic link library (DLL)), ktorú **sa pokúša proces alebo používateľ zaviesť** a porovnať túto informáciu k zoznamu autorizovaných a neautorizovaných aplikácií alebo knižníc.

- **Analýza sieťovej premávky.** Toto je často podobné činnosti sieťových IDPS. Navyše analýz sieťových, transportných a aplikačných protokolových vrstiev, môžu agenti zahrnúť do bežných aplikácií zvláštne spracovanie, ako sú napríklad e-mailoví klienti. Analýza premávky tiež umožňuje agentovi extrahovať súbory zaslané aplikáciou, akou je e-mail, web a peer-to-peer zdieľanie súborov, ktorá potom môžu byť kontrolovaná škodlivý kód.
- **Filtrácia sieťovej premávky.** Agenti často obsahujú hostovú bezpečnostnú bránu (firewall), ktorá môže obmedziť prichádzajúcu a odchádzajúcu premávku pre každú aplikáciu v systéme, zabraňujúc neoprávnenému prístupu a porušovaniu politiky akceptovateľného používania (napr. používanie nevhodných externých služieb).
- **Monitorovanie súborového systému.** Monitorovanie súborového systému je možné vykonávať pomocou niekoľkých rôznych techník, vrátane tých, ktoré sú uvedené nižšie. Administrátori by mali byť vedomí toho, že niektoré produkty vykonávajú monitorovanie na základe mien súborov, to znamená, že keď používateľ alebo útočník zmení meno súboru, techniky monitorovania súborového systému sa stanú neúčinné.
  - **Kontrola integrity súboru.** Jedná sa o pravidelné vytváranie kontrolného súčtu kritických súborov a porovnávanie kontrolného súčtu s referenčnými hodnotami a zisťovanie rozdielov. Kontrola integrity súborov zistí, že súbor bol modifikovaný.
  - **Kontrola atribútov súboru.** Jedná sa o pravidelnú kontrolu atribútov dôležitých súborov, ako je vlastníctvo a oprávnenia, na zmeny. Podobne ako kontrola integrity súborov aj tento mechanizmus zistí, že došlo k zmene.
  - **Pokusy o prístup k súboru.** Agent s podložkou na súborový systému môže monitorovať všetky pokusy o prístup ku kritickým súborom, ako sú napríklad systémové binárne súbory, a môže zastaviť podozrivé pokusy. Agent má **súbor politík týkajúcich sa prístupu k súborom**, takže agent porovná tieto politiky ku charakteristikám súčasného pokusu, vrátane toho, ktorý používateľ alebo aplikácia sa pokúša o prístup ku každému súboru, a aký typ prístupu bolo požiadané (čítanie, zápis, vykonanie). Toto by mohlo byť použité na prevenciu pred inštaláciou niektorých foriem škodlivého kódu, ako sú rootkity a trójske kone, rovnako ako na prevenciu pred mnohými ďalšími typmi škodlivých aktivít zahrňujúcich prístup k súborom, modifikácie, náhrady alebo odstránenie.

Hostové IDPS

- **Analýza záznamov.** Niektorí agenti môžu monitorovať a analyzovať operačný systém a aplikačné záznamy s cieľom identifikovať škodlivé aktivity. Tieto záznamy môžu obsahovať informácie o:
  - **udalostiach v systéme**, ktoré sú prevádzkové akcie vykonané zložkami operačného systému (napr. vypnutie systému, odštartovanie služby)
  - **auditné záznamy**, ktoré obsahujú informácie o bezpečnostných udalostiach, ako sú úspešné a neúspešné pokusy o autentizáciu a zmeny bezpečnostnej politiky
  - **aplikačných udalostiach**, ktoré sú významné prevádzkové akcie vykonané aplikáciami, ako sú štart a odstavenie aplikácie, chyby aplikácie a zásadné zmeny konfigurácie aplikácie.
- **Monitorovanie sieťovej konfigurácie.** Niektorí agenti môžu monitorovať aktuálnu konfiguráciu siete hosta a detegovať jej zmenu. Typicky sú monitorované všetky sieťové rozhranie na hostovi vrátane drôtových, bezdrôtových a virtuálnych privátnych sietí (VPN). Príklady významných zmien konfigurácie siete sú sieťové rozhrania **nastavené do promiskuitného režimu, používanie dodatočných portov TCP alebo UDP porty na hostovi, alebo používanie dodatočných sieťových protokolov ako sú nové protokoly IP**. Tieto zmeny môžu indikovať, že host už bol kompromitovaný, a je konfigurovaný na použitie pri budúcich útokoch alebo na prenos údajov.

- Vzhľadom k tomu, že hostové IDPS majú často rozsiahle znalosti o vlastnostiach a konfigurácii hostov, môže agent hostových IDPS často určiť, **či sa útok, pokiaľ nebude zastavený, proti hostovi podarí**. Agenti môžu použiť túto znalosť na výber preventívnych opatrení a priradiť alertom zodpovedajúce priority.
- **Možnosti prevencie** – Agenti hostových IDPS ponúkajú rôzne možnosti prevencie proti prienikom. Vzhľadom k tomu, že možnosti sa menia podľa použitých detekčných techník každého produktu, uvedené položky opisujú možnosti podľa detekčných techník.
  - **Analýza kódu.** Techniky analýzy kódu môžu zabrániť vykonaniu kódu, vrátane škodlivého kódu a neautorizovaných aplikácií. Niektoré hostové IDPS tiež možu zastaviť sieťové aplikácie pred zavolaním shellu, ktorý by mohol byť použitý na pokus o vykonanie určitých typov útokov. V prípade dobrej konfigurácie a dobrému vyladeniu hostového IDPS, analýza kódu môže byť veľmi efektívna, zvlášť pri zastavení doposiaľ neznámych útokov.

Hostové IDPS

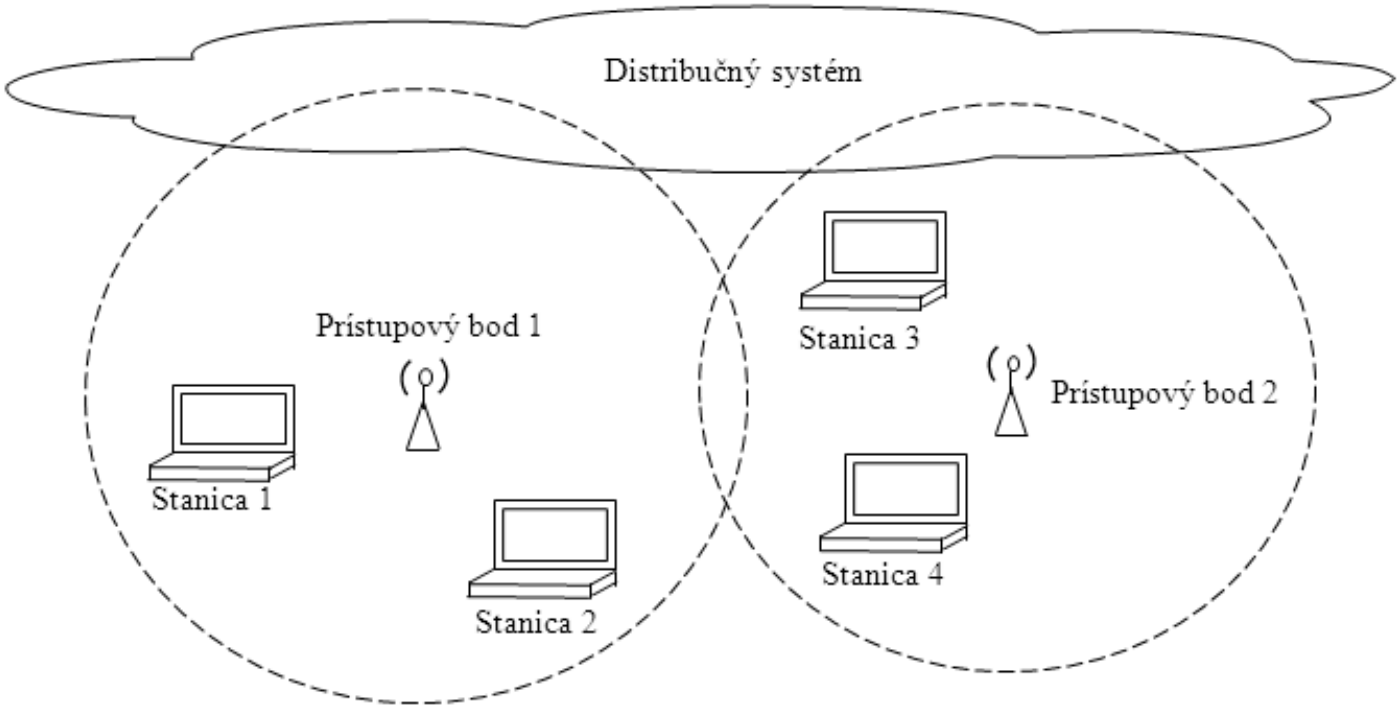
- **Analýza sieťovej premávky.** Môže **zastaviť** prichádzajúce sieťovú premávku **pred spracovaním** na hostovi a odchádzajúcu sieťovú premávku **pred jej poslaním**. Toto môže byť vykonané s cieľom zastavenia útokov na vrstve sieťovej, transportnej a aplikačnej (a v niektorých prípadoch, útoky na bezdrôtový sieťový protokol), rovnako ako zastaviť používanie nepovolených aplikácií a protokolov. Analýza môže tiež **identifikovať sťahované alebo prenášané škodlivé súbory** a zabrániť týmto súborom, aby boli uložené na hosta. Sieťová premávka zastavená alebo odmietnutá a personálna bezpečnostná brána hosta (ktorá by mohla byť vstavaná do agenta) by mohla byť rekonfigurovaná s cieľom vyhnúť sa ďodatočnej premávky týkajúcej sa podozrivého premávky. Analýza sieťovej premávky je efektívna pri zastavení mnoho známych a predtým neznámych útokov.
- **Filtrovanie sieťovej premávky.** Pracuje ako hostová bezpečnostná brána, môže **zastaviť** neoprávnený prístup a porušovanie politiky akceptovateľného použitia (napr. používanie nevhodných externých služieb). Je účinné len na zastavenie aktivity, ktorá je identifikovateľná adresou IP a portom TCP, portom UDP alebo typom a kódom ICMP.
- **Monitorovanie súborového systému.** Môže zabrániť, aby boli súbory pristúpené, modifikované alebo odstránené, čo by mohlo zastaviť inštaláciu škodlivého kódu vrátane trójskych koní a rootkitov, rovnako ako iné útoky zahŕňajúce nevhodný prístup k súborom. Táto technika môže poskytnúť ďalšiu vrstvu riadenia prístupu na doplnenie existujúcich technológií na riadenie prístupu na hostovi.

Hostové IDPS

- **Ďalšie možnosti** – Niektoré hostové IDPS ponúkajú non-IDPS možnosti ako antivírusový softvér, filtrovanie spamu a filtrovanie obsahu webu alebo e-mailu. Príklady ďalších možností sú tieto:
  - **Obmedzenie vymeniteľných médií.** Niektoré produkty môžu vynútiť obmedzenie používania výmenných médií ako sú flash disky. To môže zabrániť škodlivému kódu alebo iným nežiaducim súborom, aby boli prenesené na hosta a je tiež možné zastaviť kopírovanie citlivých súborov z hosta na vymeniteľné médiá.
  - **Monitorovanie audiovizuálnych zariadení.** Niekoľko produktov hostových IDPS môže detegovať, kedy sú aktivované alebo požité audiovizuálne zariadenia hosta. To by mohlo indikovať, že host bol napadnutý útočníkom.
  - **Bezpečnostné utesnenie (hardening) hosta.** Niektoré hostové IDPS môžu hostov automaticky priebežne bezpečnostne utesniť. Napríklad v prípade, že aplikácia je rekonfigurovaná a rekonfigurácia spôsobí vypnutie určitých bezpečnostných funkcií, IDPS môže detegovať túto skutočnosť a bezpečnostné funkcie môže aktivovať.
  - **Monitorovanie stavu procesov.** Niektoré produkty monitorujú stav procesov alebo služieb vykonávajúcich sa na hostovi a ak detegujú, že sa jeden zastavil, znovu ho automaticky reštartujú. Niektoré produkty môžu tiež monitorovať stav bezpečnostných programov ako je antivírusový softvér.
  - **Sanácia sieťovej premávky.** Niektorí agenti, zvlášť nasadený na zariadeniach, môžu sanovať monitorovanú sieťovú premávku. Napríklad, agent na zariadení môže fungovať ako proxy a prestaviť každú žiadosť a odpoveď, ktorá ním prechádza. To môže byť efektívne pri neutralizácii určitých nezvyčajných aktivít, najmä v hlavičkách paketov a hlavičkách aplikačného protokolu. Sanácia vykonaná zariadením môže tiež znížiť množstvo prieskumov, ktoré útočníci môžu vykonávať na chránených hostoch. Príklady predstavujú skrývanie odtlačkov operačných systémév serverov a správ aplikačných chýb. Niektoré produkty môžu tiež chrániť citlivé informácie, ako sú čísla sociálneho poistenia a čísla kreditných kariet, ktoré sú zobrazené na stránkach webových servera.

Bezdrôtové IDPS

- **Bezdrôtové IDPS** – monitorujú bezdrôtovú sieťovú premávku a analyzujú jej bezdrôtové sieťové protokoly s cieľom identifikovať podozrivé aktivity zahrňujúce samotné protokoly.
- WLAN (bezdrôtové LAN) podľa štandardu IEEE 802.11 majú dva základné architektonické komponenty:
  - **Stanicu (STA).** Stanica je bezdrôtové koncové zariadenie. Typickým príkladom STA je laptop, smartfón, tablet a ďalšie zariadenia spotrebnej elektroniky s vybavením podľa IEEE 802.11.
  - **Prístupový bod (AP – Access Point).** Prístupový bod logicky pripája STA k distribučnému systému, ktorý typicky je drôtovaná infraštruktúra spoločnosti. Distribučný systém je prostriedok prostredníctvom ktorého môžu STA komunikovať s drôtovanou LAN spoločnosti a externou sieťou ako je internet. Príklad architektúry bezdrôtovej LAN je na obrázku.



Bezdrôtové IDPS

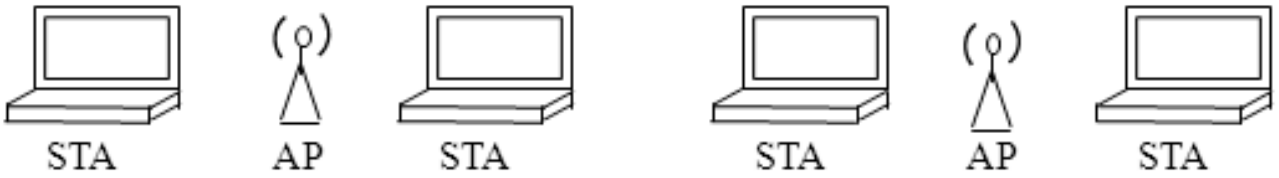
- Niektoré WLAN používajú tiež **bezdrôtové prepínače** (wireless switch):
  - Je to zariadenie, ktoré funguje ako prostredník medzi AP a distribučným systémom
  - Účelom tohto prepínača je napomáhať administrátorovi v spravovaní WLAN infraštruktúry
  - Vo WLAN bez bezdrôtových prepínačov sú AP pripojené priamo na distribučnú systém.
- Štandard IEEE 802.11 tiež definuje tieto dve WLAN architektúry:
  - **Ad hoc režim.** Ad hoc režim nevyužíva AP. Ad hoc režim, tiež známy ako peer-to-peer režim, zahrňuje dve alebo viac STA komunikujúcich priamo jeden s druhým. Známym prípadom tohto režimu sú siete MANET (Mobile Ad-hoc NETwork).
  - **Infraštruktúrny režim.** Prístupový bod logicky pripája STA k distribučnému systému, ktorý je typicky drôtovaná sieť.
- Takmer všetky WLAN sa využívajú v infraštruktúrnom režime:
  - Každý modul AP v sieti WLAN má priradené meno, ktoré sa nazýva identifikátor množiny služieb **SSID** (Service Set Identifier). SSID umožňuje STA odlíšiť jednu WLAN od druhej WLAN.
  - AP vysiela SSID vo **formáte obyčajného textu**, takže každé prijímajúce bezdrôtové zariadenie sa môže ľahko dozvedieť SSID každej WLAN, ktorá je v dosahu zariadenia.
- Hrozby proti WLAN:
  - Bezdrôtová aj pevná (drôtovaná) sieť čelia rovnakým všeobecným typom hrozieb, relatívne riziko niektorých hrozieb sa však výrazne líši. Napríklad bezdrôtové útoky zvyčajne vyžadujú, aby útočník alebo útočníkove zariadenie bolo v **tesnej fyzickej blízkosti k bezdrôtovej sieti**, na druhej strane mnoho útokov na drôtovej siete možno vykonávať na diaľku z ľubovoľného miesta. Navyše, mnoho WLAN je nastavených tak, že **nevyžadujú autentizáciu** alebo vyžadujú len slabé formy autentizácie, čo značne uľahčuje útočníkom vykonávať niekoľko typov útokov, napríklad útok man-in-the-middle.
  - Väčšina hrozieb proti WLAN zahrňujú útočníka s prístupom k rádiovému spojenie medzi STA a AP (alebo medzi dvoma STA v režime ad hoc). Mnoho útokov sa spolieha na **možnosť útočníka zachytiť sieťovú komunikácie alebo vložiť do komunikácie ďalšie správy**. To dokumentuje najvýznamnejší rozdiel medzi ochranou bezdrôtovej a drôtovej siete LAN: relatívna jednoduchosť prístupu a zmena sieťovej komunikácie.

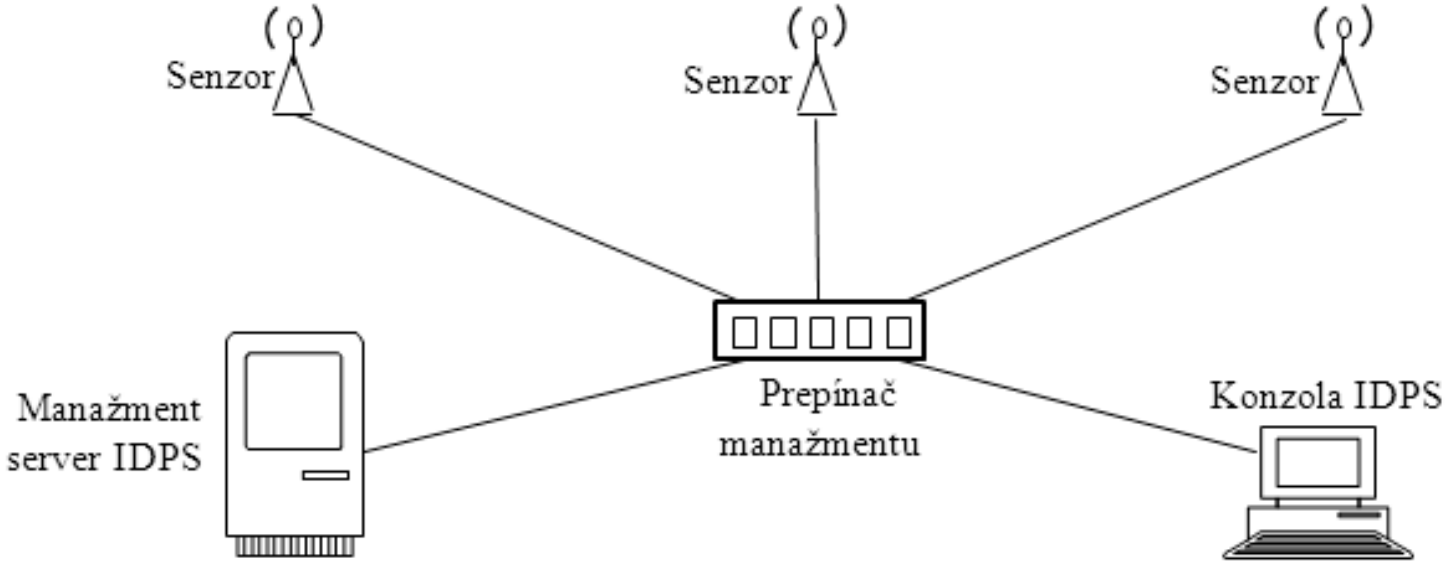
Bezdrôtové IDPS

- **Typické komponenty** – bezdrôtových IDPS sú rovnaké ako v sieťových IDPS: konzola, databázové servery (voliteľne), servery manažmentu a senzory.
  - Všetky komponenty okrem senzorov majú v podstate rovnaké funkcie pre oba typy IDPS. Bezdrôtové senzory majú rovnakú základnú úlohu ako sieťové senzory IDPS, ale **fungujú veľmi odlišne** z dôvodu zložitosti monitorovania bezdrôtovej komunikácie.
  - Na rozdiel od sieťových IDPS, ktoré môžu vidieť všetky pakety siete, bezdrôtové IDPS pracujú na princípe vzorkovania premávky. Existujú dve frekvenčné pásma na monitorovanie (2,4 GHz a 5 GHz) a každé pásmo je rozdelená do kanálov. Senzor nemôže monitorovať všetku premávku v pásme naraz, v danom čase môže monitorovať iba jeden kanál. Aby sa potlačil tento handicap, senzory často prepínajú medzi monitorovanými kanálmi. Tomuto mechanizmu sa hovorí **skenovanie kanálov** (senzor monitoruje každý kanál niekoľkokrát za sekundu).
- **Bezdrôtové senzory** sú dostupné vo viacerých formách:
  - **Venované.** Venovaný senzor je zariadenie, ktoré vykonáva funkcie bezdrôtového IDPS, ale neprenáša sieťovú premávku od zdroja k cieľu. Venované senzory sú často úplne pasívne a iba odchytávajú sieťovú premávku, ktorú majú v danom kanály v dosahu. Niektoré špecializované senzory vykonávajú analýzu premávky samy, zatiaľ čo ostatné senzory iba preposielajú sieťovú premávku na analýzu na server manažmentu. Senzor je typicky pripojený k drôtovej sieti. Venované senzory sú zvyčajne navrhnuté na jeden z dvoch typov nasadenia:
    - **Pevný senzor** - je nasadený na určitom mieste. Tieto senzory sú typicky závislé od infraštruktúry spoločnosti (napr. energie, drôtová sieť). Pevné senzory sú obvykle zariadenia.
    - **Mobilný senzor** - je určený na použitie v pohybe. Napríklad bezpečnostný správca môže používať mobilný senzor pri prechádzkach po budove spoločnosti a hľadať škodlivé AP. Mobilné senzory sú buď zariadenia alebo sú softvér inštalovaný na notebooku s bezdrôtovým NIC, schopným vykonávať RF monitorovanie.
  - **V spojení s AP.** Niekoľkí výrobcovia pridali funkcie IDPS do AP. Takýto AP zvyčajne zabezpečuje menšie možnosti detekcie ako venovaný senzor, pretože AP sa musí rozdeliť s existujúcim výpočtovým výkonom na zabezpečenie prístupu do siete a monitorovanie viacerých kanálov alebo pásiem na škodlivé aktivity. Ak IDPS monitoruje iba jedno pásmo a kanál, potom spojené riešenie môže poskytnúť rozumnú bezpečnosť a sieťovú dostupnosť. V prípade, že IDPS musí monitorovať viaceré pásma alebo kanály, potom potreba senzora vykonávať skenovanie kanálov môže prerušiť funkciu AP a tým spôsobiť jeho **dočasnú nedostupnosť** ne jeho primárnom pásme a kanále.
  - **V spojení s bezdrôtovým prepínačom.** Niektoré bezdrôtové prepínače tiež ponúkajú niektoré funkcie bezdrôtových IDPS ako sekundárne funkcie. Bezdrôtové prepínače obvykle **neposkytujú také detekčné schopnosti** ako v spojení s AP alebo venované senzory.

Bezdrôtové IDPS

- **Architektúry sietí** – Komponenty bezdrôtových IDPS sú typicky vzájomne prepojené prostredníctvom drôtovej siete (viď obrázok). Podobne ako pri sieťových IDPS, môže byť na komunikáciu medzi komponentmi IDPS využitá štandardná (produkčná) sieť spoločnosti alebo oddelená sieť manažmentu. Niektoré bezdrôtové senzory IDPS (mobilné senzory) sú používané samostatne a nepotrebujú drôtovú sieťovú konektivitu.





Bezdrôtové IDPS

- **Bezpečnostné možnosti** – Bezdrôtové IDPS poskytujú niekoľko typov bezpečnostných funkcií. Pretože bezdrôtové IDPS je relatívne nová forma IDPS, ich možnosti sa medzi výrobcami v súčasnej dobe veľmi líši.
- **Možnosti zbierania informácií** – Väčšina bezdrôtových IDPS môže zbierať informácie o bezdrôtových zariadeniach. Príklady možností zbierania týchto informácií sú tieto:
  - **Identifikovanie zariadení WLAN.** Väčšina senzorov IDPS dokáže vytvoriť a udržiavať zoznam spozorovaných zariadení WLAN, vrátane AP, bezdrôtových klientov a ad hoc (peer-to-peer) klientov. Zoznam je zvyčajne založený na SSID a adries MAC bezdrôtových zariadení (bezdrôtových sieťových kariet). Niektoré senzory môžu využívať techniku odtlačkov (fingerprint) v pozorovanej premávke na verifikáciu výrobcu namiesto spoliehania sa na adresu MAC, ktorá môže byť sfalšovaná. Zoznam sa dá využiť ako profil na identifikáciu nových zariadení WLAN a odstránenie existujúcich zariadení.
  - **Identifikovanie WLAN.** Väčšina senzorov IDPS sleduje pozorované siete WLAN identifikujúc ich podľa SSID. Správcovia potom môžu označiť každú položku v zozname sietí ako autorizovanú WLAN, neškodnú susednú WLAN (napr. ďalšej spoločnosti v tej istej budove) alebo škodlivú WLAN. Tieto informácie môžu byť použité na identifikáciu nových WLAN, rovnako ako priorizácia reakcia na zistené udalosti.
- **Možnosti zaznamenania** – Bezdrôtové IDPS zvyčajne vykonávajú rozsiahle zaznamenanie údajov týkajúcich sa detegovaných udalostí. Tieto údaje možno použiť na potvrdenie platnosti alertov, vyšetrovanie incidentov a na koreláciu udalostí medzi IDPS a ďalších záznamových zdrojov. Údajové polia, zvyčajne zaznamenané pomocou bezdrôtových IDPS, obsahujú toto:
  - Časová pečiatka (zvyčajne dátum a čas)
  - Typ udalosti alebo alertu
  - Priradenie priority a závažnosti
  - Zdrojová adresa MAC (výrobca je často identifikovaný podľa adresy)
  - Číslo kanála
  - ID senzoru, ktorý spozoroval udalosť
  - Vykonané preventívne akcie (ak nejaké boli).

Bezdrôtové IDPS

- **Možnosti detekcie** – Bezdrôtové IDPS dokáže detegovať útoky, chybné konfigurácie a porušovania politiky na úrovni protokolu WLAN, a to predovšetkým skúmanie komunikačného protokolu IEEE 802.11 . Bezdrôtové IDPS neskúmajú komunikáciu na vyšších úrovniach (napr. adresy IP, aplikačný payload). Niektoré produkty vykonávajú iba jednoduchú detekciu príznakov, zatiaľ čo iné používajú kombináciu mechanizmu príznakov, mechanizmu anomálií a mechanizmu analýzy stavových protokolov.
- **Typy detegovaných udalostí** – Typy udalostí, ktoré sú najčastejšie detegované bezdrôtovými senzormi IDPS, pokrývajú:
  - **Neoprávnené WLAN a zariadenia WLAN.** Prostredníctvom svojich možností zbierania informácií, väčšina bezdrôtových senzorov IDPS sú schopné detegovať škodlivé AP, neoprávnené STA a neoprávnené WLAN (infraštruktúrny a ad hoc režim).
  - **Slabo zabezpečené zariadenia WLAN.** Väčšina bezdrôtových senzorov IDPS je schopná identifikovať AP a STA, ktoré nepoužívajú náležité bezpečnostné opatrenia. To zahŕňa detegovanie chybných konfigurácií a použitie slabých protokolov WLAN a implementácií protokolu. Dosiahne sa to tak, že senzor identifikuje odchýlky od špecifických politík spoločnosti ako sú nastavenie šifrovania, autentizácie, prenosovej rýchlosti, mien SSID a kanálov. Senzor napríklad by mohol detegovať, že STA používa šifrovanie WEP namiesto WPA2 alebo IEEE 802.11i. Väčšina typov udalostí, ktoré môžu byť detegované bezdrôtovými IDPS spadajú do tejto kategórie detekcie.
  - **Nezvyčajné vzory použitia.** Niektoré senzory používajú mechanizmus anomálií na detekciu nezvyčajných vzorov použitia WLAN. Ak napríklad oveľa viac STA ako obvykle používa konkrétny AP alebo je oveľa vyššie než obvykle množstvo sieťovej premávky medzi STA a AP, jedno zo zariadení mohlo byť kompromitované alebo neoprávnená strana by mohla využívať WLAN. Mnoho senzorov je schopných identifikovať neúspešné pokusy o pripojenie sa do siete WLAN.
  - **Používanie bezdrôtových sieťových skenerov** (napr. nástrojov war driving). Tieto skenery sa používajú na identifikáciu nezabezpečených alebo slabo zabezpečených sietí WLAN. Bezdrôtové IDPS môžu detegovať iba používanie aktívnych skenerov (skenery generujúce premávku bezdrôtovej siete). Nemôžu detegovať využívanie pasívnych senzorov, ktoré iba jednoducho monitorujú a analyzujú pozorovanú premávku.

Bezdrôtové IDPS

- **Podmienky a útoky Denial of Service (DoS)** (napr. rušenia siete). DoS útoky zahrňujú logické útoky ako sú **záplavy** (flooding), ktorá predstavuje súčasné posielanie veľkého množstva správ na AP a fyzické útoky ako je **rušenie** (jamming), ktorá predstavuje vyžarovanie elektromagnetickej energie na frekvenciách siete WLAN tak, aby sa frekvencia stala pre WLAN nepoužiteľná. DoS útoky môžu byť často detegovaný pomocou mechanizmov stavovej analýzy protokolu a metódou anomálií. Tieto mechanizmy môžu stanoviť, či pozorovaná aktivita je v súlade s očakávanou aktivitou. Mnoho útokov DoS je detekovaných napočítavaním udalostí počas určitého časového obdobia a alertom keď počet udalostí prekročí prahové hodnoty. Napríklad, veľký počet udalostí týkajúci sa ukončenia bezdrôtových sieťových relácií, môže indikovať útok DoS.
- **Impersonifikácia a útoky man-in-the-middle.** Niektoré bezdrôtové senzory IDPS môžu detegovať prípad, keď zariadenie sa snaží sfalšovať identitu iného zariadenia. Tento prípad môže byť zistený tak, že senzor identifikuje rozdiely v charakteristikách aktivity ako sú napríklad určité hodnoty v rámcoch.

- Väčšina bezdrôtových senzorov IDPS je schopná identifikovať fyzické umiestnenie detegovanej hrozby pomocou **triangulácie** – odhadnutím približnej vzdialenosti hrozby od viacerých senzorov na základe sily signálu hrozby, ktorý prijíma každý senzor a následným výpočtom fyzického miesta (odhadované vzdialenosť od každého senzora), na ktorom by hrozba mala byť umiestnená. Určenie fyzickej lokácie hrozby umožňuje spoločnosti poslať pracovníkov fyzickej ochrany na riešenie hrozby. Produkty bezdrôtových IDPS na základe plánu podlažia budovy sú schopné stanoviť či je hrozba vo vnútri alebo mimo budovy alebo ak je na verejnom priestranstve alebo v zabezpečenej oblasti. Táto informácia je užitočná nielen pri hľadaní a pre zastavenie hrozby, ale aj pri priorizácii reakcii na túto hrozbu. Bezdrôtové senzory IDPS môžu nastaviť prioritu alertov čiastočne na základe umiestnenie každej hrozby. Ručné senzory IDPS možno tiež použiť na určenie polohy hrozby, najmä ak pevné senzory neponúkajú možnosti triangulácie alebo v prípade, že hrozba je v pohybe.

Bezdrôtové IDPS

- **Možnosti prevencie** – senzory bezdrôtových IDPS ponúkajú dva typy možností prevencie pred prienikmi:
  - **Bezdrôtové.** Niektoré senzory sú schopné vzduchom **ukončiť spojenia** medzi škodlivým alebo chybne konfigurovaným STA a autorizovaným AP alebo medzi oprávneným STA a škodlivým alebo chybne konfigurovaným AP. Senzory túto aktivitu zabezpečia zaslaním správy koncovým bodom komunikácie, aby de-asociovali aktuálnu reláciu. Senzor potom odmieta, aby bolo povolené nadviazanie nového spojenia.
  - **Drôtové.** Niektoré senzory môžu dať pokyn prepínaču na drôtovej sieti, aby **zablokoval sieťovú aktivitu zahŕňajúce konkrétne STA alebo AP** a to podľa adresy MAC zariadenia alebo portu prepínača. Ak STA napríklad posiela útoky na server v pevnej sieti, senzor môže dať pokyn drôtovému prepínaču, aby blokoval všetku aktivitu na a z tohto STA. Táto technika je účinná iba pre blokovanie škodlivého STA alebo AP v komunikácii drôtovej sieti. Technika nezastaví STA alebo AP od ďalšieho vykonávania škodlivých aktivít prostredníctvom bezdrôtových protokolov.
- Väčšina senzorov IDPS umožňujú administrátorom špecifikovať konfiguráciu prevenčných možností pre každý typ alertu. Zvyčajne to zahrňuje povolenie alebo blokovanie prevencie, ako aj to, ktoré typy prevenčných možností by mali byť použité. Niektoré senzory IDPS majú režim učenia alebo simulácie, ktorý potláčajú všetky preventívne opatrenia a namiesto toho indikujú, kedy by boli vykonané prevenčné akcie. Tento režim umožňuje administrátorom monitorovať a doladiť konfiguráciu prevenčných možností pred povolením prevencie, čo znižuje riziko vykonávanie preventívnych opatrení na neškodné aktivity.
- Dôležitým aspektom je efekt, ktoré preventívne opatrenia môže mať na monitorovaný senzor. Ak snímač napríklad vysiela signály na ukončenie spojení, nemôže vykonávať skenovanie kanálov s cieľom monitorovanie sledovania ďalšej komunikácie, pokiaľ neukončí preventívnu akciu. Pre zmiernenie tohto efektu niektoré **senzory majú dve rádiá**: jedno na monitorovanie a detekciu a druhé na vykonávanie preventívnych opatrení.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™